

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S62	4	((MASUE) near2 (SHIBA)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2007/05/18 14:21
S63	106	((SHINICHI) near2 (KAWAMURA)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2007/05/18 14:21
S64	13	((SHINICHI) near2 (KAWAMURA)).INV. and adder	US-PGPUB; USPAT; USOCR	OR	ON	2007/05/18 14:18
S65	110	S62 S63 S64	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:18
S66	1374	380/28.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:19
S67	137	708/7.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:19
S68	44	708/135.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:19
S69	292	708/492.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:19
S70	114	708/501.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:19
S71	83	708/503.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:19
S72	191	708/523.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:19
S73	177	708/603.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:19
S74	571	708/620.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:19
S75	2821	S66 S67 S68 S69 S70 S71 S72 S73 S74	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:19
S76	1374	380/28.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:20
S77	137	708/7.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:20

EAST Search History

S78	44	708/135.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:20
S79	292	708/492.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:20
S80	114	708/501.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:20
S81	83	708/503.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:20
S82	191	708/523.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:20
S83	177	708/603.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:20
S84	571	708/620.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:20
S85	11	(S76 S77 S78 S79 S80 S81 S82 S83 S84) and (integer and finite and adder).clm.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/05/18 14:20
S86	6	((MASUE) near2 (SHIBA)).INV.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT ; IBM_TDB	OR	ON	2007/05/18 14:21
S87	525	((SHINICHI) near2 (KAWAMURA)).INV.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT ; IBM_TDB	OR	ON	2007/05/18 14:21
S88	17	(S86 S87) and (adder)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT ; IBM_TDB	OR	ON	2007/05/18 14:23
S89	1	(S86 S87) and (integer and finite)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT ; IBM_TDB	OR	ON	2007/05/18 14:24

[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#)

Welcome United States Patent and Trademark Office

[Search Session History](#)[BROWSE](#)[SEARCH](#)[IEEE XPLORE GUIDE](#)

Fri, 18 May 2007, 2:36:50 PM EST

Edit an existing query or
compose a new query in the
Search Query Display.

Search Query Display

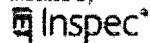
Select a search number (#)
to:

- Add a query to the Search Query Display
- Combine search queries using AND, OR, or NOT
- Delete a search
- Run a search

Recent Search Queries

- #1 ((cryptography <and> integer <and> finite)<in>metadata)
- #2 dual <and> cryptography <in> (ti)
- #3 (integer <and> (finite <or> galois) <and> multiplier<IN>metadata)
- #4 (((integer <and> (finite <or> galois) <and> multiplier) <in>metadata)) <and> (pyr >= 1950 <and> pyr <= 1999)
- #5 (((integer <and> (finite <or> galois) <and> multiplier) <in>metadata)) <and> (pyr >= 1950 <and> pyr <= 1999)
- #6 (((integer <and> (finite <or> galois) <and> multiplier) <in>metadata)) <and> (pyr >= 1950 <and> pyr <= 1999)
- #7 (((integer <and> (finite <or> galois) <and> multiplier) <in>metadata)) <and> (pyr >= 1950 <and> pyr <= 1999)
- #8 (((integer <and> (finite <or> galois) <and> multiplier) <in>metadata)) <and> (pyr >= 1950 <and> pyr <= 1999)
- #9 (((integer <and> (finite <or> galois) <and> multiplier) <in>metadata)) <and> (pyr >= 1950 <and> pyr <= 1999)
- #10 (((integer <and> galois <and> selector)<in>metadata)) <and> (pyr >= 1950 <and> pyr <= 1999)

indexed by

[Help](#) [Contact Us](#) [Privacy & ;](#)

© Copyright 2006 IEEE --


[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) |

Welcome United States Patent and Trademark Office

☐ Search Results

BROWSE

SEARCH

IEEE XPLORE GUIDE

Results for "((cryptography <and> integer <and> finite)<in>metadata)"

☐ e-mail

Your search matched 16 of 1568664 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

» Search Options

[View Session History](#)[New Search](#)

Modify Search

((cryptography <and> integer <and> finite)<in>metadata)

☐ Check to search only within this results set
Display Format: ☒ Citation ☐ Citation & Abstract

» Key

IEEE JNL IEEE Journal or Magazine

IET JNL IET Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IET CNF IET Conference Proceeding

IEEE STD IEEE Standard

 [Select All](#) [Deselect All](#)

- ☐ 1. **Evaluating instruction set extensions for fast arithmetic on binary finite fi**
 Fiskiran, A.M.; Lee, R.B.;
[Application-Specific Systems, Architectures and Processors, 2004. Proceeding International Conference on](#)
 2004 Page(s):125 - 136
 Digital Object Identifier 10.1109/ASAP.2004.1342464
 AbstractPlus | Full Text: PDF(355 KB) IEEE CNF
[Rights and Permissions](#)
- ☐ 2. **The unreasonable effectiveness of number theory in science and commu**
Rayleigh Lecture)
 Schroeder, M.R.;
[ASSP Magazine, IEEE \[see also IEEE Signal Processing Magazine\]](#)
 Volume 5, Issue 1, Jan. 1988 Page(s):5 - 12
 Digital Object Identifier 10.1109/53.661
[AbstractPlus](#) | Full Text: PDF(924 KB) IEEE JNL
[Rights and Permissions](#)
- ☐ 3. **On the list and bounded distance decodibility of Reed-Solomon codes**
 Qi Cheng; Daqing Wan;
[Foundations of Computer Science, 2004. Proceedings. 45th Annual IEEE Sym](#)
 17-19 Oct. 2004 Page(s):335 - 341
 Digital Object Identifier 10.1109/FOCS.2004.46
[AbstractPlus](#) | Full Text: PDF(176 KB) IEEE CNF
[Rights and Permissions](#)
- ☐ 4. **Instruction set extension for fast elliptic curve cryptography over binary 1**
(2/sup m/)
 Groszschadl, J.; Kamendje, G.-A.;
[Application-Specific Systems, Architectures, and Processors, 2003. Proceedin](#)
[International Conference on](#)
 24-26 June 2003 Page(s):455 - 468
[AbstractPlus](#) | Full Text: PDF(1180 KB) IEEE CNF
[Rights and Permissions](#)
- ☐ 5. **The parallel improved Lanczos method for integer factorization over finit**
public key cryptosystems
 Yang, L.T.; Brent, R.P.;

[Parallel Processing Workshops, 2001. International Conference on 3-7 Sept. 2001](#) Page(s):106 - 111

Digital Object Identifier 10.1109/ICPPW.2001.951908

[AbstractPlus](#) | Full Text: [PDF](#)(504 KB) IEEE CNF

[Rights and Permissions](#)

6. **Public-key cryptography using paraunitary matrices**
Delgosha, F.; Fekri, F.;
[Signal Processing, IEEE Transactions on \[see also Acoustics, Speech, and Signal Processing, IEEE Transactions on\]](#)
Volume 54, Issue 9, Sept. 2006 Page(s):3489 - 3504
Digital Object Identifier 10.1109/TSP.2006.877670
[AbstractPlus](#) | Full Text: [PDF](#)(616 KB) IEEE JNL
[Rights and Permissions](#)
7. **On the sphere-decoding algorithm I. Expected complexity**
Hassibi, B.; Vikalo, H.;
[Signal Processing, IEEE Transactions on \[see also Acoustics, Speech, and Signal Processing, IEEE Transactions on\]](#)
Volume 53, Issue 8, Part 1, Aug. 2005 Page(s):2806 - 2818
Digital Object Identifier 10.1109/TSP.2005.850352
[AbstractPlus](#) | Full Text: [PDF](#)(488 KB) IEEE JNL
[Rights and Permissions](#)
8. **Attacking ElGamal based cryptographic algorithms using Pollard's rho algorithm**
Haraty, R.A.; Otrok, H.; Nasser Kassar, A.;
[Computer Systems and Applications, 2005. The 3rd ACS/IEEE International Conference on](#)
2005 Page(s):91
Digital Object Identifier 10.1109/AICCSA.2005.1387082
[AbstractPlus](#) | Full Text: [PDF](#)(1104 KB) IEEE CNF
[Rights and Permissions](#)
9. **Algorithm engineering for public key algorithms**
Beth, T.; Gollman, D.;
[Selected Areas in Communications, IEEE Journal on](#)
Volume 7, Issue 4, May 1989 Page(s):458 - 466
Digital Object Identifier 10.1109/49.17708
[AbstractPlus](#) | Full Text: [PDF](#)(740 KB) IEEE JNL
[Rights and Permissions](#)
10. **Comment on 'Cryptanalysis of public key distribution systems based on polynomials' and reply**
Burmester, M.; Da-Xing Li;
[Electronics Letters](#)
Volume 27, Issue 22, 24 Oct. 1991 Page(s):2042
[AbstractPlus](#) | Full Text: [PDF](#)(88 KB) IET JNL
11. **Soft-Timeout Distributed Key Generation for Digital Signature based on Elliptic Curve Logarithm for Low-Power Devices**
Caimu Tang; Chronopoulos, A.T.; Raghavendra, C.S.;
[Security and Privacy for Emerging Areas in Communications Networks, 2005. First International Conference on](#)
05-09 Sept. 2005 Page(s):353 - 364
Digital Object Identifier 10.1109/SECURECOMM.2005.52
[AbstractPlus](#) | Full Text: [PDF](#)(384 KB) IEEE CNF
[Rights and Permissions](#)
12. **Use of Sparse and/or Complex Exponents in Batch Verification of Exponentiation**
Jung Hee Cheon; Dong Hoon Lee;

[Computers, IEEE Transactions on](#)
Volume 55, Issue 12, Dec. 2006 Page(s):1536 - 1542
Digital Object Identifier 10.1109/TC.2006.207
[AbstractPlus](#) | [Full Text: PDF\(1082 KB\)](#) IEEE JNL
[Rights and Permissions](#)

- ┐ **13. Lower bounds on the linear complexity of the discrete logarithm in finite**
Meidl, W.; Winterhof, A.;
[Information Theory, IEEE Transactions on](#)
Volume 47, Issue 7, Nov. 2001 Page(s):2807 - 2811
Digital Object Identifier 10.1109/18.959261
[AbstractPlus](#) | [References](#) | [Full Text: PDF\(297 KB\)](#) IEEE JNL
[Rights and Permissions](#)
- ┐ **14. A timing-and-area tradeoff GF(p) elliptic curve processor architecture for**
Wu Shuhua; Zhu Yuefei;
Communications, Circuits and Systems, 2005. Proceedings. 2005 International
Volume 2, 27-30 May 2005 Page(s):
Digital Object Identifier 10.1109/ICCCAS.2005.1495347
[AbstractPlus](#) | [Full Text: PDF\(317 KB\)](#) IEEE CNF
[Rights and Permissions](#)
- ┐ **15. Research on computing IP core for the digital signature algorithm**
Jianpeng Chu; Yongsheng Xu; Xiaojin Li; Zongsheng Lai;
[ASIC, 2003. Proceedings. 5th International Conference on](#)
Volume 2, 21-24 Oct. 2003 Page(s):1329 - 1331 Vol.2
[AbstractPlus](#) | [Full Text: PDF\(221 KB\)](#) IEEE CNF
[Rights and Permissions](#)
- ┐ **16. Hardware architectures proposed for cryptosystems based on hyperellip**
Wollinger, T.; Paar, C.;
[Electronics, Circuits and Systems, 2002. 9th International Conference on](#)
Volume 3, 15-18 Sept. 2002 Page(s):1159 - 1162 vol.3
Digital Object Identifier 10.1109/ICECS.2002.1046458
[AbstractPlus](#) | [Full Text: PDF\(310 KB\)](#) IEEE CNF
[Rights and Permissions](#)